

JUDGE CAPRONI

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF NEW YORK

U.S. Securities and Exchange Commission,

*Plaintiff,*

v.

Case No. \_\_\_\_\_

Iat Hong, Bo Zheng, and Hung Chin,

*Defendants,*

and

Sou Cheng Lai,

*Relief Defendant.*

16 CV 9947

MEMORANDUM OF LAW IN SUPPORT OF  
SECURITIES AND EXCHANGE COMMISSION'S *EX PARTE* APPLICATION FOR  
TEMPORARY RESTRAINING ORDER AND ANCILLARY EQUITABLE RELIEF

## TABLE OF CONTENTS

I.	STATEMENT OF FACTS.....	2
A.	Defendants.....	2
B.	Relief Defendant .....	4
C.	Hacked Law Firms .....	4
D.	Summary of Securities Traded By Defendants .....	5
E.	Defendants’ Trading Strategy Focuses on Upcoming M&As .....	6
F.	Defendants Target Law Firm 1 as A Source Of Material Nonpublic M&A Information.....	6
G.	Law Firm 1 Is Hacked.....	7
H.	Defendants Hong And Zheng Trade In InterMune Based On Material Nonpublic Information Stolen From Law Firm 1 And Reap Significant Illegal Profits .....	8
I.	Defendants Use Additional Confidential Information Stolen From Law Firm 1 To Trade .....	10
J.	Defendants Trade In Altera Based On Material Nonpublic Information Stolen From Law Firm 1’s Network And Reap Significant Illegal Profits.....	11
K.	Law Firm 2 Is Hacked.....	13
L.	Defendants Hong and Chin Trade In Borderfree Based On Material Nonpublic Information Stolen From Law Firm 2 And Reap Significant Illegal Profits .....	15
M.	Defendants Are Connected To An Additional Hack Using The Same Internet Protocol Addresses Associated With The Law Firm 1 And Law Firm 2 Hacks .....	16
N.	Defendants Trade in Additional Securities Linked To Law Firm 2.....	17
II.	LEGAL ARGUMENT .....	18
A.	The SEC Makes “A Proper Showing” For Entry Of A Temporary Restraining Order .....	19
1.	The SEC Makes A Prima Facie Case That Defendants Violated §10(b) And Rule 10b-5.....	20
2.	The SEC Makes A Prima Facie Case That Defendants Hong and Chin Violated § 14(e) And Rule 14e-3.....	27
3.	The SEC Demonstrates A Reasonable Likelihood That Defendants Will Commit Future Violations Of The Securities Laws .....	29
B.	The SEC Makes The Showing Required To Freeze Defendants’ And Relief Defendant’s Assets.....	30

C. A Repatriation Order Is Necessary And Appropriate Because There Is Good Cause To Believe That Defendants And Relief Defendant Have Assets Outside The United States .....32

D. An Expedited Discovery Order Is Necessary And Appropriate .....34

E. An Order Prohibiting Destruction Of Documents Is Necessary And Appropriate...35

F. An Order Permitting Alternative Service Of Process Is Necessary And Appropriate .....36

III. CONCLUSION .....38

## TABLE OF AUTHORITIES

**Cases**

<i>Exp.-Imp. Bank v. Asia Pulp &amp; Paper Co., Ltd.</i> , 2005 WL 1123755 (S.D.N.Y. May 11, 2005).....	39
<i>F.T.C. v. Pecon Software Ltd.</i> , 2013 WL 4016272 (S.D.N.Y. Aug. 7, 2013).....	38
<i>Heyman v. Heyman</i> , 356 F. Supp. 958 (S.D.N.Y. 1973).....	22
<i>Richter v. Achs</i> , 962 F. Supp. 31 (S.D.N.Y. 1997).....	21
<i>Rio Properties, Inc. v. Rio Int'l Interlink</i> , 284 F.3d 1007 (9th Cir.2002).....	37
<i>SEC v. American Bd. of Trade, Inc.</i> , 830 F.2d 431 (2d Cir. 1987).....	31
<i>SEC v. Anticevic</i> , 2009 WL 361739 (S.D.N.Y. Feb. 13, 2009).....	19, 37, 38
<i>SEC v. Apuzzo</i> , 689 F.3d 204 (2d Cir. 2012).....	22
<i>SEC v. Aragon Capital Advisors, LLC</i> , 2011 WL 3278642 (S.D.N.Y. July 26, 2011).....	19
<i>SEC v. Babikian</i> , 2014 WL 2069348 (S.D.N.Y. Apr. 21, 2014).....	35
<i>SEC v. Byers</i> , 2009 WL 33434 (S.D.N.Y. Jan. 7, 2009).....	31
<i>SEC v. Cavanagh</i> , 1 F. Supp. 2d 337 (S.D.N.Y. 1998).....	18, 20
<i>SEC v. Cavanagh</i> , 155 F.3d 129 (2d Cir.1998).....	18, 32
<i>SEC v. Cavanagh</i> , 1998 WL 132842 (S.D.N.Y. Mar. 23, 1998).....	36
<i>SEC v. Cobalt Family Investors I, LLC</i> , 2011 WL 4899909 (S.D.N.Y. June 14, 2011)....	19, 35, 36
<i>SEC v. Dorozhko</i> , 574 F.3d 42 (2009).....	22, 23
<i>SEC v. Gonzalez de Castilla</i> , 145 F. Supp. 2d 402 (S.D.N.Y. June 27, 2001).....	35
<i>SEC v. Heden</i> , 51 F. Supp. 2d 296 (S.D.N.Y.1999).....	31
<i>SEC v. Illarramendi</i> , 2011 WL 2457734 (D. Conn. June 16, 2011).....	33, 34
<i>SEC v. Infinity Grp. Co.</i> , 212 F.3d 180 (3d Cir. 2000).....	31
<i>SEC v. Maillard</i> , 2014 WL 1660024 (S.D.N.Y. Apr. 23, 2014).....	31

<i>SEC v. Management Dynamics, Inc.</i> , 515 F.2d 801 (1975) .....	30
<i>SEC v. Materia</i> , 745 F.2d 197 (2d. Cir. 1984) .....	18, 19, 29, 31, 36
<i>SEC v. Mayhew</i> , 121 F.3d 44 (2d Cir. 1997).....	29
<i>SEC v. McGinnis</i> , 2013 WL 6500461 (D. Conn, Dec. 11, 2013).....	36
<i>SEC v. Pentagon Capital Management PLC</i> , 725 F.3d 279 (2d Cir. 2013).....	21
<i>SEC v. Shehyn</i> , 2008 WL 6150322 (S.D.N.Y. Nov. 26, 2008) .....	37
<i>SEC v. Softpoint, Inc.</i> , 958 F. Supp. 846 (S.D.N.Y. 1997).....	21
<i>SEC v. Straub</i> , 921 F.Supp.2d 244 (S.D.N.Y. 2013).....	22
<i>SEC v. Unifund SAL</i> , 910 F.2d 1028 (2d Cir.1990).....	18, 31
<i>SEC v. Universal Consulting Res. LLC</i> , 2010 WL 4873733 (D. Colo. Nov. 23, 2010).....	34
<i>SEC v. Warde</i> , 151 F.3d 42 (2d Cir. 1998).....	28
<i>Smith v. SEC</i> , 653 F.3d 121 (2011) .....	32
<i>United States v. Chestman</i> , 947 F.2d 551 (1991) .....	28
<i>United States v. O'Hagan</i> , 521 U.S. 642 (1997) .....	28

## **Statutes**

15 U.S.C. § 78j(b).....	20
15 U.S.C. § 78n(e) .....	27
15 U.S.C. § 78t(b).....	22
15 U.S.C. § 78t(e).....	21
15 U.S.C. § 78u(d)(1) .....	18
15 U.S.C. § 78u(d)(5) .....	18

## Other Authorities

Hague Convention, art. 10(a), Nov. 15, 1965, 20 U.S.T. 361 .....	37
Reservations, Declarations, and Understandings for the Special Administrative Region of Hong Kong and the Special Administrative Region of Macao, Hague Convention, available at, <a href="https://www.hcch.net/en/instruments/conventions/statustable/notifications/?csid=393&amp;disp=resn">https://www.hcch.net/en/instruments/conventions/statustable/notifications/?csid=393&amp; disp=resn</a> (last visited Oct. 25, 2016) .....	37

## Rules

17 C.F.R. § 240.10b-5.....	20, 21
17 C.F.R. § 240.14e-3(a) .....	27
Fed. R. Civ. P. 26(d)(1) .....	34
Fed. R. Civ. P. 4(f)(2)(C).....	37
Fed. R. Civ. P. 4(f)(2)(C)(ii).....	36
Fed. R. Civ. P. 4(f)(3) .....	35
Fed. R. Civ. P. 65(b)(2) .....	33

**MEMORANDUM OF LAW IN SUPPORT OF  
SECURITIES AND EXCHANGE COMMISSION'S *EX PARTE* APPLICATION FOR  
TEMPORARY RESTRAINING ORDER AND ANCILLARY EQUITABLE RELIEF**

Pursuant to Federal Rule of Civil Procedure 65(b), Plaintiff Securities and Exchange Commission ("SEC" or "Commission") seeks emergency equitable relief to halt a fraudulent hacking-to-trade scheme involving three Chinese nationals — Iat Hong ("Hong"), Bo Zheng ("Zheng"), and Hung Chin ("Chin") (collectively "Defendants") — who have reaped approximately \$3 million in illegal profits by trading on stolen material nonpublic information.

Specifically, on multiple occasions from at least July 31, 2014 through August 2015, Defendants directly, indirectly, or through or by means of others hacked into the nonpublic networks of two New York-headquartered law firms and secretly copied and removed emails of certain law firm partners to obtain confidential information about corporate transactions for which the law firms were providing representation. Defendants then used this confidential information to trade ahead of mergers and acquisitions ("M&A") announcements involving three companies: InterMune, Inc., Altera Corporation, and Borderfree, Inc.

Defendants' hacking-to-trade scheme violated the Securities Exchange Act of 1934 (the "Exchange Act") and Commission rules enacted thereunder. Specifically, Defendants violated the antifraud provisions in § 10(b) and Rule 10b-5. Alternatively, the Defendants committed secondary violations of § 10(b) and Rule 10b-5 and/or primary violations of § 20(b). Additionally, Defendants Hong and Chin violated § 14(e) and Rule 14e-3. To stop Defendants from further violations of the federal securities laws, the Commission respectfully requests a temporary restraining order, asset freeze, repatriation order, expedited discovery, preservation order, and alternative service of process. The requested equitable relief is necessary and appropriate and should be granted for the reasons set forth below.

## I. STATEMENT OF FACTS

### A. Defendants

Iat Hong (“Hong”) is 26 years old and resides in the Macau Special Administrative Region of the People’s Republic of China (“Macau”) (Sachar Decl. ¶10, Ex. B).

Defendant Hong used four brokerage accounts in connection with the hacking-to-trade scheme. Three of these four accounts were held at Interactive Brokers, Inc., a U.S. online brokerage firm. Defendant Hong accessed the Interactive Brokers accounts through corresponding accounts at Hong Kong-based broker-dealer Sun Hung Kai Investment Services, Inc. (“SHK”), with account numbers ending \*3220, \*3255, and \*3506 via an introducing relationship that SHK had with Interactive Brokers (Sachar Decl. ¶¶8, 19, 20). Of the three accounts, one was a cash account in his name with an Interactive Brokers account number ending in \*6749 (“Hong cash account”), while the other two accounts were in his mother’s name, Sou Cheng Lai: (i) a cash account used from approximately April 2014 through December 2014 with an Interactive Brokers account number ending in \*5376; and (ii) a margin account used beginning in approximately January 2015 with an Interactive Brokers account number ending in \*2615 (collectively “Hong/Lai accounts”) (Sachar Decl. ¶¶10, 17, 18). Defendant Hong had full trading authority over the Hong/Lai accounts and controlled them (Sachar Decl. ¶¶22, 24, Exs. J and K). The fourth account used in the scheme was an account held in Defendant Hong’s name with an account number ending in \*1999 at BOCI Securities Limited (“BOCI”), a Hong Kong-based broker-dealer (Sachar Decl. ¶13, Ex. E). On his BOCI account application, Defendant Hong represented that his employer was a Chinese company whose name was translated as “Zhuhai City Smart Airflow Co., Ltd.” and describes the nature of the company’s business as “IT,” which upon information and belief, reflects the common English abbreviation for “Information Technology (Sachar Decl. ¶13, Ex. E). Defendant Hong was able to access the



U.S. markets in the BOCI account through BOCI's U.S.-based clearing firm (Sachar Decl. ¶15). Defendant Hong made approximately \$1.4 million in illegal profits from his participation in the fraudulent scheme.

Bo Zheng ("Zheng") is 30 years old and resides in Changsha, China (Sachar Decl. ¶27, Ex. M). Defendant Zheng obtained a Master of Science in Petroleum Engineering from the University of Tulsa in approximately 2010 (Sachar Decl. ¶25). Defendant Zheng used three brokerage accounts in his name in connection with the fraudulent scheme: an online Scottrade cash account ending in \*0256; a BOCI margin account ending in \*1975; and a CMB Int'l Securities Ltd. ("CMB") account ending in \*2716 (Sachar Decl. ¶¶26, 27, 29). CMB, like BOCI, is a Hong Kong-based broker-dealer. For the BOCI and CMB accounts, Defendant Zheng was able to access the U.S. markets through BOCI's and CMB's respective U.S.-based clearing firms (Sachar Decl. ¶31). On his BOCI account application, Defendant Zheng represented that his employer was a Chinese company whose name was translated as "Zhuhai City Aijia Smart Airflow Co., Ltd." and describes the nature of the company's business as "IT," which upon information and belief, reflects the common English abbreviation for "Information Technology" (Sachar Decl. ¶28). Defendant Zheng opened his BOCI account on the same day that Defendant Hong opened his BOCI account (compare dates at Sachar Decl. ¶¶14, 28, Exs. E and M). Defendant Zheng made approximately \$500,000 in illegal profits from his participation in the fraudulent scheme.

Hung Chin ("Chin") is 50 years old and resides in either Hong Kong or Macau (Sachar Decl. ¶34, Ex. P). His address in Macau is identical to that of Hong and his mother, Relief Defendant Sou Cheng Lai (Sachar Decl. ¶34, Exs. F, B, and P). According to brokerage records, Defendant Chin is the Chief Executive Officer of a Chinese company, and describes the nature of

the company's business as "IT," which, upon information and belief, reflects the common English abbreviation for "Information Technology" (Sachar Decl. ¶35, Ex. P). Defendant Chin used a BOCI account ending in \*6696 in his own name in connection with the fraudulent scheme. Defendant Chin was able to access the U.S. markets through BOCI's U.S.-based clearing firm (Sachar Decl. ¶15). Defendant Chin made slightly over \$1 million in illegal profits from his participation in the fraudulent scheme.

**B. Relief Defendant**

Sou Cheng Lai ("Lai") is 47 years old and resides in Macau (Sachar Decl. ¶17, Ex. F page 1 and Ex. G page 3). She is Defendant Hong's mother (Sachar Decl. ¶22, Ex. J). Lai is named as a Relief Defendant because her accounts received illegal profits from Defendant Hong's trading as part of the fraudulent scheme.

**C. Hacked Law Firms**

Law Firm 1 is headquartered in New York City with offices throughout the United States, Europe, and Asia (Sachar Decl. ¶37). Law Firm 1 is well-known for providing representation in connection with M&A activity. Here, Law Firm 1 provided representation on at least two transactions where — when the transactions were announced — the companies' share prices surged dramatically. During the relevant period, Partner A was a Partner in Law Firm 1's Manhattan offices and chaired Law Firm 1's M&A practice group (Sachar Decl. ¶37).

Law Firm 2 is headquartered in New York City with an overseas office (Sachar Decl. ¶38). Law Firm 2 is well-known for providing representation in connection with M&A activity. Here, Law Firm 2 provided representation on at least one transaction where — when the transaction was announced — the company's share price surged dramatically. During the relevant period, Partner B was a Partner in Law Firm 2's Manhattan offices and chaired Law Firm 2's corporate practice group (Sachar Decl. ¶38).

**D. Summary of Securities Traded By Defendants**

Between August 13, 2014 and August 21, 2014, Defendants Hong and Zheng purchased a total of 18,000 shares of InterMune, Inc. (“InterMune”). InterMune was a California-based biotechnology company that was listed on the NASDAQ under the ticker symbol ITMN (Sachar Decl. ¶53). InterMune was acquired by Roche Holding AG in a deal that was announced on August 24, 2014. Partner A and Law Firm 1 provided representation to a party that expressed interest in acquiring InterMune during the relevant time period. Defendants sold all of their InterMune shares by August 25, 2014 for a combined profit of over \$393,000.

Defendants purchased a total of over 207,000 shares of Altera Corporation (“Altera”) from February 17, 2015 to March 27, 2015. Altera was a California-based computer chip manufacturer that was listed on the NASDAQ under the ticker symbol ALTR (Sachar Decl. ¶71). Altera merged with Intel Corporation in a deal that was announced on June 1, 2015 (Sachar Decl. ¶87). Rumors of the merger surfaced in the media on March 27, 2015. Partner A and Law Firm 1 provided representation in connection with the Intel-Altera merger. By April 15, 2015, Defendants sold all of the above-described 207,000 Altera shares for a combined profit of over \$1.63 million.

Between April 29, 2015 and May 5, 2015, Defendants purchased 113,000 shares in Borderfree, Inc. (“Borderfree”), which was a Manhattan-based e-commerce company that was listed on the NASDAQ under the ticker symbol BRDR (Sachar Decl. ¶97). Pitney Bowes, Inc. (“Pitney Bowes”) acquired Borderfree in a tender offer that was announced on May 5, 2015. Partner B and Law Firm 2 provided representation in connection with the tender offer. Defendants sold all of their Borderfree shares by May 19, 2015 for a combined profit of approximately \$850,000.

**E. Defendants' Trading Strategy Focuses on Upcoming M&As**

As early as March 2014, Defendants Hong and Zheng communicated about trading in U.S.-listed stocks and noted that M&A announcements would cause a company's stock price to increase considerably. Specifically, Defendant Zheng emailed a PowerPoint presentation to Defendant Hong on March 28, 2014. The presentation was titled "Internal Information of US Stock Operations" and explained that "[t]he goal is to improve US stock operations and to seize the right time to buy and sell stocks" (Sachar Decl. ¶¶41, 42, Ex. R, page 1). One of the slides explicitly stated that "[w]e should focus on a company's . . . M&A news . . . , which usually would cause the stock price to fluctuate significantly within a short period" (Sachar Decl. ¶¶41, 42, Ex. R, page 2).

This same Power Point presentation also contained a slide indicating that Defendants Zheng and Hong had nonpublic information about certain companies. For example, one of the slides noted that a particular company had several new technology products that had not yet been released to the public and explicitly identified one product that the company planned to announce in the 2014-2015 timeframe (Sachar Decl. ¶¶41, 42, Ex. R, page 27).

**F. Defendants Target Law Firm 1 as A Source Of Material Nonpublic M&A Information**

Defendants identified Law Firm 1 as a source of material nonpublic information about M&A transactions. On July 21, 2014, Defendant Zheng sent Defendant Hong an email with a Chinese subject that translates to "[Law Firm 1] analysis template," and attached a spreadsheet (Sachar Decl. ¶¶43, 44, Ex. S). The spreadsheet contained information about two M&A transactions that were completed in 2012 (*Id.*). Law Firm 1 and Partner A were included as representing parties involved in the deals (*Id.*). The spreadsheet also listed stock prices for the companies involved in the deals, including their prices immediately before and immediately after

the deals were made public (*Id.*). On July 29, 2014, Defendant Hong emailed Defendant Chin a Word document titled “New York.docx” (Sachar Decl. ¶¶45, 46, Ex. T). The document listed the names of eleven partners at Law Firm 1 in Law Firm 1’s New York, Washington, D.C., Silicon Valley, and Hong Kong offices (*Id.*). All but one of the partners was in Law Firm 1’s M&A or private equity practice groups (Sachar Decl. ¶45). Partner A was first on the list (*Id.*).

#### **G. Law Firm 1 Is Hacked**

By no later than July 31, 2014, Defendants directly, indirectly, or through or by means of others hacked into Law Firm 1’s nonpublic network through deceptive means that included:

- ***Installing malware on servers in Law Firm 1’s network.*** “Malware” is software that is intended to damage or disable computers and computer networks, or to circumvent installed security and access controls. The malware was used to obtain broad access to nonpublic aspects of Law Firm 1’s network, including Law Firm 1’s nonpublic email systems (Sachar Decl. ¶¶47, 48).
- ***Compromising the user account of a Law Firm 1 Information Technology employee (“Law Firm 1 IT Employee”), and posing as that employee.*** Law Firm 1 IT Employee had exceptional credentials that gave him access to all other email accounts within Law Firm 1’s nonpublic network, including the email accounts of Law Firm 1 M&A partners (such as Partner A) (Sachar Decl. ¶¶47, 49).
- ***Concealing their breach of Law Firm 1’s nonpublic network by disguising their activities as typical network traffic.*** As a result, Law Firm 1’s security systems did not recognize the deceptive breach of Law Firm 1’s nonpublic network (Sachar Decl. ¶¶47, 50).

Through the hack, Defendants directly, indirectly, or through or by means of others stole approximately 6.05 gigabytes of data from Law Firm 1's nonpublic network on the evening of July 31, 2014 and the morning of August 1, 2014, which is equivalent to approximately 605,000 pages of Law Firm 1 data, and transmitted that data to a remote internet location (Sachar Decl. ¶¶47, 51). From August 1, 2014 through September 12, 2014, Defendants directly, indirectly, or through or by means of others stole approximately 53 gigabytes more of data from Law Firm 1's nonpublic network — the equivalent of approximately 5.3 million pages — and transmitted that data to a remote internet location (Sachar Decl. ¶¶47, 52).

**H. Defendants Hong And Zheng Trade In InterMune Based On Material Nonpublic Information Stolen From Law Firm 1 And Reap Significant Illegal Profits**

Defendants Hong and Zheng used the material nonpublic information stolen from Law Firm 1 to trade in InterMune. Information concerning a potential acquisition of InterMune was contained in Partner A's emails at the time data was stolen from Law Firm 1. In June 2014, a pharmaceutical company retained Law Firm 1 and Partner A to provide representation in connection with a confidential bid to acquire InterMune (Sachar Decl. ¶¶47, 54). On August 1, 2014, the pharmaceutical company's Chief Executive Officer ("CEO") contacted InterMune's CEO to express the pharmaceutical company's interest in acquiring all of InterMune's shares in an all-cash transaction (Sachar Decl. ¶¶47, 55). The pharmaceutical company then confirmed its interest in an August 4, 2014 letter that stated a specific price-per-share (\$67 per share) that the pharmaceutical company was willing to pay for InterMune (Sachar Decl. ¶¶47, 56). Partner A received the letter in his Law Firm 1 email account as an attachment to an August 7, 2014 email from the pharmaceutical company (Sachar Decl. ¶57). The following day, Partner A used his Law Firm 1 email account to exchange emails with the pharmaceutical company about the

potential InterMune bid (*Id.*). These emails included specific information about the price-per-share that had been offered (*Id.*).

Defendants Hong and Zheng had this material nonpublic information when they traded in InterMune. Beginning on August 13, 2014, Defendant Hong — using both the Hong cash account and Hong/Lai account — purchased shares of InterMune (Sachar Decl. ¶58, Ex. Q InterMune summary). From approximately 10:45 a.m. ET through 12:32 p.m. ET on August 13, 2014, Hong purchased 7,500 InterMune shares for approximately \$360,000 (*Id.*).

Minutes after Defendant Hong completed his purchase of 7,500 InterMune shares on August 13, 2014, various news services reported that InterMune was working with financial advisers to evaluate strategic options as it braced itself for potential takeover interest from larger drug makers (Sachar Decl. ¶59, Ex. U). The reports identified the pharmaceutical company represented by Law Firm 1 and Partner A as a potential acquirer (*Id.*). The news reports caused InterMune's stock price to increase by approximately \$5 per share, or approximately 11% (Sachar Decl. ¶60, Ex. Q InterMune summary). The news reports did not, however, discuss the price-per-share that the pharmaceutical company Law Firm 1 represented had offered for InterMune (Sachar Decl. ¶61, Ex. U). Moreover, neither InterMune nor the pharmaceutical company confirmed the accuracy of the reports (Sachar Decl. ¶61). Therefore, the material nonpublic information that Defendant Hong and Defendant Zheng had concerning InterMune remained both material and nonpublic. Defendant Hong purchased an additional 1,000 InterMune shares in the Hong/Lai account on August 13 after the news reports were published (Sachar Decl. ¶61, Ex. Q InterMune summary).

Beginning late on August 16 and continuing into August 17, Defendants directly, indirectly, or through or by means of others stole approximately ten gigabytes of data from Law



Firm 1's nonpublic network, which translates to approximately one million pages (Sachar Decl. ¶62). The next day, August 18, 2014, Defendant Hong purchased an additional 4,500 InterMune shares in the Hong/Lai account (Sachar Decl. ¶63, Ex. Q InterMune summary). Defendant Zheng joined him by purchasing 850 InterMune shares in his CMB account on that day (*Id.*). On August 19, 2014, both Defendants Zheng and Hong purchased more InterMune shares — with Defendant Zheng purchasing 950 shares in his CMB account and Defendant Hong purchasing 400 shares in the Hong cash account (*Id.*). On August 21, 2014, Defendant Hong purchased an additional 2,800 InterMune shares in the Hong cash account (*Id.*).

In total — from August 13 through August 21 — Defendants Hong and Zheng purchased 18,000 InterMune shares, spending over \$920,000 to do so (*Id.*).

On August 24, 2014, InterMune announced that it had been acquired by Roche Holding AG, a German pharmaceutical company in an all cash transaction at \$74 per share (Sachar Decl. ¶64, Ex. V). InterMune's stock price increased by approximately \$19 per share, or approximately 40% (Sachar Decl. ¶65, Ex. W). Defendants Hong and Zheng subsequently sold their combined 18,000 InterMune shares for total illegal profits of approximately \$393,000. (Sachar Decl. ¶66, Ex. Q). In particular, Defendant Hong illegally profited by over \$355,000, and Defendant Zheng illegally profited by approximately \$35,000 (*Id.*).

#### **I. Defendants Use Additional Confidential Information Stolen From Law Firm 1 To Trade**

The same day that Defendant Hong began purchasing InterMune shares, he also began purchasing shares in a biopharmaceutical company and an entertainment company (Sachar Decl. ¶¶67, 68, Ex. X). Five days later, Defendant Hong purchased shares in a specialty pharmaceutical company (*Id.*). Defendants Zheng and Chin also purchased shares in some of



these companies. For example, Defendants traded in the biopharmaceutical company until December 2014 (*Id.*).

The biopharmaceutical company, the entertainment company, the specialty pharmaceutical company, and InterMune had one thing in common: Law Firm A was providing confidential M&A representation for possible transactions involving each of the companies (Sachar Decl. ¶69). While none of these other three companies ever consummated the M&A transactions for which Law Firm 1 provided representation, Defendants — upon information and belief — traded in these companies based on stolen information from Law Firm 1 concerning potential deals involving these companies (*Id.*).

**J. Defendants Trade In Altera Based On Material Nonpublic Information Stolen From Law Firm 1's Network And Reap Significant Illegal Profits**

Between January 7, 2015 and February 9, 2015, Defendants directly, indirectly, or through or by means of others continued to access Law Firm 1's nonpublic network through deceptive means and stole data containing confidential material nonpublic information and transmitted that data to a remote internet location (Sachar Decl. ¶70). Defendants then used material nonpublic information to unlawfully trade in Altera, reaping enormous profits.

Intel retained Law Firm 1 to represent it as lead M&A counsel in confidential discussions to acquire Altera (Sachar Decl. ¶71, Ex. Y). Partner A served as the lead partner on this representation (Sachar Decl. ¶72). On January 29, 2015, Partner A received in his Law Firm 1 email account the final version of a January 27, 2015 letter from Intel to Altera in which Intel expressed an interest in acquiring Altera (Sachar Decl. ¶73). That letter included specific pricing information (*Id.*). After January 29, 2015, Partner A represented Intel in confidential material nonpublic discussions concerning the transaction (Sachar Decl. ¶74, Ex. Y). On February 2, 2015, for example, Partner A participated in confidential discussions with Altera in which Intel

offered to purchase Altera for \$50 per share, and Altera countered with \$65 per share (Sachar Decl. ¶74, Ex. Y page 7). On February 4, 2015, Partner A met with Intel and its advisors concerning how to respond to Altera's \$65 per share counterproposal (Sachar Decl. ¶75, Ex. Y page 9). On February 8, 2015, Partner A exchanged emails with Intel representatives in which they continued to discuss a purchase price (Sachar Decl. ¶76).

Beginning on February 17, 2015, Defendants made substantial and aggressive purchases of Altera based on the material nonpublic information noted above. From February 17, 2015 to March 27, 2015, Defendants purchased a total of over 207,000 Altera shares for approximately \$7.5 million (Sachar Decl. ¶77, Ex. Q Altera broad summary of trading). Moreover — on the twenty-nine trading days in the February 17, 2015 to March 27, 2015 time period — Defendants purchased Altera stock on every trading day except for two (Sachar Decl. ¶77, Ex. Q Detailed summary of Altera trading).

Throughout this period, Defendants wired significant amounts of money into their respective brokerage accounts to fund this massive trading (Sachar Decl. ¶¶78, 79, 80, 82, 83, 84, 85, 86, Exs. Z, AA, and BB). But even with those significant wires of money into the accounts, Defendants bought large amounts of Altera shares on margin (Sachar Decl. ¶¶78, 79, 81, 82, 83, 84, 85, 86, Exs. Z, AA, and BB). “Buying on margin” is the practice of borrowing money to purchase securities, and as such, can be extremely risky because, if the price of the securities goes down, the borrower might have to come up with substantial additional cash to cover the margin loan. Buying on margin also subjects a trader to additional costs such as the interest payment for use of the borrowed money.

In fact, Defendant Hong (in the Hong/Lai account) — on three separate occasions — traded so heavily in Altera that he exceeded the permissible amounts he was allowed to borrow.

(Sachar Decl. ¶81, Ex. Z). As a result, the brokerage firm automatically sold approximately \$130,000 worth of Altera shares from the account to bring it into margin compliance (Sachar Decl. ¶81, Ex. Z). Defendants Zheng and Chin similarly engaged in margin trading in their respective BOCI accounts to purchase Altera stock (Sachar Decl. ¶¶82, 83, 84, 85, 86, Exs. AA and BB).

On March 27, 2015, various news services reported that Intel and Altera were in confidential merger discussions (Sachar Decl. ¶87, Ex. CC). On the announcement, Altera's stock price increased approximately \$9 per share, or about 30% (Sachar Decl. ¶88, Ex. DD).

By April 15, 2015, Defendants sold all of the above-described 207,000 Altera shares for total illegal profits nearing \$1.63 million (Sachar Decl. ¶89, Ex. Q Altera Trading Summaries). In particular, Defendant Hong illegally profited by approximately \$600,000; Defendant Chin illegally profited by approximately \$600,000; and Defendant Zheng illegally profited by over \$450,000.

#### **K. Law Firm 2 Is Hacked**

On or about April 6, 2015, Defendants directly, indirectly, or through or by means of others hacked into Law Firm 2's nonpublic network through deceptive means that included:

- *Compromising the user account and password of a Law Firm 2 Information Technology employee ("Law Firm 2 IT employee").* The compromised credentials were used to pose as Law Firm 2 IT employee on the network and gain access Law Firm 2's broader nonpublic network (Sachar Decl. ¶¶90, 91).
- *Placing malware on a Law Firm 2 web server ("Law Firm 2 web server").* That malware then gave the Law Firm 2 web server commands to download additional

malware to the Law Firm 2 web server and store that malware in memory (Sachar Decl. ¶¶90, 92).

- ***Compromising a Law Firm 2 administrator account that was used to operate and manage Law Firm 2's email server.*** An “administrator account” is an account that allows authorized persons to make changes to network systems that will affect other users. Authorized users of administrator accounts can, for example, change security settings, install software and hardware, and access all aspects of a nonpublic network. Here, the compromised credentials allowed access to Law Firm 2's email server, including the email account of Partner B who headed Law Firm 2's corporate practice group (Sachar Decl. ¶¶90, 93).
- ***Concealing the breach of Law Firm 2's nonpublic network by disguising the activities as harmless and ordinary.*** This included disguising malware as a routine Google update service and renaming the stolen email files so that they looked like files containing ordinary network graphics (Sachar Decl. ¶¶90, 94).

On seven occasions from April 28, 2015 to July 31, 2015, Defendants directly, indirectly, or through or by means of others stole approximately seven gigabytes of compressed data from Law Firm 2's nonpublic network and transmitted that data to a remote internet location (Sachar Decl. ¶¶90, 95). “Compressed data” represents files that have been reduced in size to increase the speed of transmitting those files from one computer to another. Thus, the total volume of actual data taken was likely far larger than seven gigabytes, or more than 700,000 pages (*Id.*).

**L. Defendants Hong and Chin Trade In Borderfree Based On Material Nonpublic Information Stolen From Law Firm 2 And Reap Significant Illegal Profits**

Defendants directly, indirectly, or through or by means of others stole data from Law Firm 2's nonpublic network (among other dates) three times on April 28 and 29 of 2015. The specific times and amounts of data stolen in each breach are reflected in the chart below (Sachar Decl. ¶96):

Date	Time (ET)	Amount of Compressed Data
4/28/2015	10:55 p.m.	860 megabytes
4/29/2015	1:22 a.m.	380 megabytes
4/29/2015	1:35 a.m.	76 megabytes

At the time of the first breach on April 28, 2015, Law Firm 2 represented Pitney Bowes in final-stage tender offer discussions to acquire Borderfree (Sachar Decl. ¶97). Pitney Bowes retained Law Firm 2 to represent it in merger and acquisition discussions (*Id.*). Partner B was the lead partner on that deal (*Id.*). Partner B's Law Firm 2 email account contained confidential material nonpublic information concerning the transaction including an April 25, 2015 email circulating a draft Exclusivity Agreement in connection with a "potential acquisition" of Borderfree by Pitney Bowes (Sachar Decl. ¶98, Ex. EE).

Defendants Hong and Chin subsequently traded in Borderfree based on the material nonpublic information stolen from Law Firm 2. On April 29, 2015 beginning at approximately 10:00 a.m. ET, Defendant Chin purchased 10,000 Borderfree shares in his BOCI account. (Sachar Decl. ¶99, Ex. FF Detailed Borderfree Summary Chart). About ninety minutes later, Defendant Hong purchased 8,000 Borderfree shares in the Hong/Lai account (*Id.*). These shares cost approximately \$120,000 total, and Defendant Hong and Chin's trades occurred less than twelve hours after data was stolen from Law Firm 2 (*Id.*).

After April 29, 2015 and continuing through May 5, 2015, Defendants Chin and Hong continued purchasing significant numbers of Borderfree shares (Sachar Decl. ¶100, Ex. FF Detailed Borderfree Summary Chart). Chin purchased his shares in his BOCI account while Hong purchased his shares in the Hong/Lai margin account (Sachar Decl. ¶99, Ex. FF Detailed Borderfree Summary Chart). Defendants Hong and Chin purchased Borderfree so aggressively that their purchases constituted a significant percentage of the stock's trading volume between April 29, 2015 and May 5, 2015 (Sachar Decl. ¶100, Ex. FF Broader Borderfree Summary Chart). In total, Defendants Hong and Chin purchased 113,000 Borderfree shares for approximately \$730,000 (*Id.*). When Borderfree announced its merger with Pitney Bowes on May 5, 2015, Borderfree's stock price increased by approximately \$7 per share — skyrocketing by approximately 105% (Sachar Decl. ¶101, 102, Exs. GG and HH).

Defendants Hong and Chin sold their Borderfree shares for a combined illegal profit of nearly \$850,000, with Hong illegally profiting by over \$418,000 and Chin illegally profiting by approximately \$430,000 (Sachar Decl. ¶103, Ex. FF).

**M. Defendants Are Connected To An Additional Hack Using The Same Internet Protocol Addresses Associated With The Law Firm 1 And Law Firm 2 Hacks**

During the relevant period, Defendants demonstrated an interest in robotic vacuums and robot engineering generally. First, Defendants exchanged numerous emails from at least June 2014 through at least June 2015 concerning robotic vacuums (Sachar Decl. ¶104, Ex. II). Second, in the spring of 2016, Defendant Hong posted to the Internet a series of videos related to robot engineering (Sachar Decl. ¶105, Ex. LL). One of these videos listed the name of a company with a virtually identical name to the employer that both Defendants Hong and Zheng listed on their respective BOCI brokerage accounts that they opened on the same day (Sachar Decl. ¶¶14, 27, 105, Exs. E, M, and LL).

By August 2014 and continuing through at least late March 2015, a U.S. Robotics Company was the victim of several computer hacking attacks (Sachar Decl. ¶106). At least one email, which was received by all three Defendants, had attachments depicting proprietary and confidential schematic designs of a robotic vacuum manufactured by the U.S. Robotics Company (Sachar Decl. ¶¶107, 108, Ex. JJ). Upon information and belief, Defendants obtained this proprietary information from the U.S. Robotics Company by directly, indirectly, or through or by means of others hacking into the nonpublic network of the U.S. Robotics Company.

The same internet protocol addresses used for the late March 2015 hack of the U.S. Robotics Company overlapped with the hacks of Law Firm 1 and Law Firm 2 (Sachar Decl. ¶109). Here, malware used in connection with the late March 2015 hack of the U.S. Robotics Company and the early April 2015 Law Firm 2 hack emanated from the *same* IP address (Sachar Decl. ¶110 a.). Moreover – in between the late March 2015 hack of the U.S. Robotics Company and the early April 2015 Law Firm 2 hack – that *same* IP address was used to interface with Law Firm 1’s nonpublic network (Sachar Decl. ¶110 b.). Furthermore, additional malware used in connection with the late March 2015 hack of the U.S. Robotics Company emanated from the *same* IP address to which stolen data was sent from the Law Firm 2 hack (Sachar Decl. ¶110 c.).

**N. Defendants Trade in Additional Securities Linked To Law Firm 2**

Prior to the Pitney Bowes/Borderfree merger announcement, Defendants Hong and Chin purchased small amounts of Pitney Bowes shares (Sachar Decl. ¶111, Ex. KK). These were in addition to the Borderfree shares Defendants purchased. Additionally, Defendants opened stock positions in seven companies from May 1, 2015 through the end of 2015. These seven companies spanned a diverse array of industries and included a book retailer, a business services company, a film production company, an oil and gas equipment manufacturer, a car rental company, an energy company, and an engineering equipment company (*Id.*).



Pitney Bowes and these seven other companies had one thing in common. They all were either existing clients of Law Firm 2 and/or companies that Law Firm 2 had represented or was representing in connection with merger and acquisition transactions (Sachar Decl. ¶112).

For example, Partner B represented Pitney Bowes in its acquisition of Borderfree. He also was involved in representing six of the seven other companies whose securities Defendants purchased (Sachar Decl. ¶113). Moreover, two of those companies were ones in which Law Firm 2 provided or was providing confidential representation in connection with merger or acquisition discussions. These companies were also from varied sectors, as one was the energy company and the other was the engineering equipment company noted above (*Id.*).

## II. LEGAL ARGUMENT

Section 21(d)(1) of the Exchange Act authorizes the SEC, “upon a proper showing,” to obtain “a temporary or permanent injunction” against “any person [who] is engaged or is about to engage in acts or practices constituting a violation” of the federal securities laws. 15 U.S.C. § 78u(d)(1). “In [the Second] Circuit, the SEC, unlike a private litigant, need not show risk of irreparable injury to obtain an injunction, nor the unavailability of remedies at law.” *SEC v. Cavanagh*, 1 F. Supp. 2d 337, 359-60 (S.D.N.Y. 1998) (citing *SEC v. Unifund SAL*, 910 F.2d 1028, 1036 (2d Cir.1990)). Rather, the SEC need make only “a substantial showing of likelihood of success as to both a current violation and the risk of repetition.” *SEC v. Cavanagh*, 155 F.3d 129, 132 (2d Cir.1998). “There need be only a reasonable likelihood that the activity complained of will be repeated” because § 21(d)(1) vests the district court with wide discretion to grant injunctive relief. *SEC v. Materia*, 745 F.2d 197 (2d. Cir. 1984).

Injunctive relief, however, is not the only remedy that the Commission may seek or the district court may grant: “the Commission may seek, and any Federal court may grant, any



equitable relief that may be appropriate or necessary for the benefit of investors.” 15 U.S.C. § 78u(d)(5). “Once the equity jurisdiction of the district court properly has been invoked, the court has power to order all equitable relief necessary under the circumstances.” *Materia*, 745 F.2d at 200. Indeed, “any form of ancillary relief may be granted where necessary and proper to effectuate the purposes of” the federal securities laws. *Id.*

The breadth of the district court’s equitable powers permits “noninjunctive relief [to] take a variety of forms[,]” *id.*, including the specific noninjunctive relief that the Commission seeks here. Asset freezes, repatriation orders, preservation orders, expedited discovery, and alternative service of process all have been ordered by this Court when necessary to effectuate the purposes of the federal securities laws. *See, e.g., SEC v. Aragon Capital Advisors, LLC*, 2011 WL 3278642, at \*11 (S.D.N.Y. July 26, 2011) (ordering asset freeze, repatriation, and expedited discovery); *SEC v. Cobalt Family Investors I, LLC*, 2011 WL 4899909, at \*1 (S.D.N.Y. June 14, 2011) (ordering preservation of documents); *SEC v. Anticevic*, 2009 WL 361739, at \*5 (S.D.N.Y. Feb. 13, 2009) (ordering alternative service of process).

The injunctive and noninjunctive ancillary relief that the Commission seeks here is necessary and appropriate. Therefore, the Commission respectfully requests that the Court exercise its equitable power to issue a temporary restraining order, asset freeze, repatriation order, preservation order, expedited discovery, and alternative service of process. The facts and circumstances that justify entry of each of these orders is set forth more fully in the sections that follow.

#### **A. The SEC Makes “A Proper Showing” For Entry Of A Temporary Restraining Order**

The “proper showing” that the SEC must make to obtain a temporary restraining order is twofold. *Cavanagh*, 1 F. Supp. 2d at 132,135. *First*, the SEC must make a prima facie case that

Defendants violated the securities laws. *Id.* ***Second***, the SEC must demonstrate a likelihood that Defendants will commit a future violation of the securities laws. *Id.* Based on the evidence as presented in the pleadings, the Commission satisfies this forward- and backward-looking test. As set forth more fully in the subsections that follow, all of the Defendants should be enjoined from, either directly or indirectly, violating § 10(b) of the Exchange Act and Rule 10b-5. Defendants further should be enjoined from violating § 20(b) of the Exchange Act. Additionally, Defendants Hong and Chin should be enjoined from violating § 14(e) of the Exchange Act and Rule 14e-3.

**1. The SEC Makes A Prima Facie Case That Defendants Violated §10(b) And Rule 10b-5**

The SEC makes a prima facie case that Defendants violated § 10(b) and Rule 10b-5, either primarily or secondarily. Section 10(b) of the Exchange Act makes it unlawful for any person to “use or employ, in connection with the purchase or sale of any security registered on a national securities exchange or any security not so registered . . . any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe.” 15 U.S.C. § 78j(b) (2012). Rule 10b-5 specifies that:

It shall be unlawful for any person, directly or indirectly, by the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange,

- (a) To employ any device, scheme, or artifice to defraud,
- (b) To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading, or
- (c) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person,

in connection with the purchase or sale of any security.

17 C.F.R. § 240.10b–5.

To establish a primary violation of § 10(b) and Rule 10b-5, the SEC must demonstrate that “a party . . . (1) made a material misrepresentation or a material omission as to which he had a duty to speak, or use[d] a fraudulent device; (2) with scienter; (3) in connection with the purchase or sale of securities. *SEC v. Pentagon Capital Management PLC*, 725 F.3d 279, 285 (2d Cir. 2013) (internal quotations omitted). Additionally, the SEC must establish that the party’s conduct is within the jurisdiction of the federal securities laws by showing “the use of any means or instrumentality of interstate commerce, or of the mails or of any facility of any national securities exchange[.]” 17 C.F.R. § 240.10b–5. “The jurisdictional requirements of Section[] 10(b) and Rule 10b–5 are broadly construed,” however. *SEC v. Softpoint, Inc.*, 958 F. Supp. 846, 865 (S.D.N.Y. 1997); *see also Richter v. Achs*, 962 F. Supp. 31, 33 (S.D.N.Y. 1997) (“[I]t is well settled that the fraud itself need not be transmitted through the jurisdictional means. All that is necessary is that the designated means be used in some phase of the transaction, which need not be the part in which the fraud occurs.”) (*quoting Heyman v. Heyman*, 356 F. Supp. 958, 969 (S.D.N.Y. 1973)). For example, “it is undisputed that the use of the Internet is an ‘instrumentality of interstate commerce.’” *SEC v. Straub*, 921 F.Supp.2d 244, 262 (S.D.N.Y. 2013).

In interpreting § 10(b) and Rule 10b-5, the Second Circuit explicitly stated that “computer hacking could be, by definition, a ‘deceptive device or contrivance’ that is prohibited by Section 10(b) and Rule 10b–5.” *SEC v. Dorozhko*, 574 F.3d 42, 51 (2009). For example, the Court recognized that “misrepresenting one’s identity in order to gain access to information that is otherwise off limits, and then stealing that information is plainly ‘deceptive’ within the ordinary meaning of the word.” *Id.*

A secondary violation of § 10(b) and Rule 10b-5 is established by demonstrating, pursuant to § 20(e) of the Exchange Act, that a party “aided and abetted” another party’s primary violation of § 10(b) and Rule 10b-5. 15 U.S.C. § 78t(e); *SEC v. Apuzzo*, 689 F.3d 204, 206 (2d Cir. 2012) (holding that aiding and abetting liability has three elements: “(1) the existence of a securities law violation by the primary (as opposed to the aiding and abetting) party; (2) ‘knowledge’ of this violation on the part of the aider and abettor; and (3) ‘substantial assistance’ by the aider and abettor in the achievement of the primary violation” and that recklessness is sufficient to satisfy the scienter requirement).

Alternatively, primary liability is established by demonstrating, pursuant to § 20(b) of the Exchange Act, that a party “acted through or by means of” another party to accomplish a violation of § 10(b) and Rule 10b-5. 15 U.S.C. § 78t(b) (making it “unlawful for any person, directly or indirectly, to do any act or thing which it would be unlawful for such person to do under the provisions of this title or any rule or regulation thereunder through or by means of any other person”).

Based on the evidence as presented in the pleadings, the SEC makes a prima facie case that Defendants committed primary violations of § 10(b) and Rule 10b-5 or alternatively, primary violations of § 20(b) and/or are secondarily liable as aiders and abettors for violations of § 10(b) and Rule 10b-5 under § 20(e).

**a. Primary Liability Under § 10(b) and Rule 10b-5**

The SEC’s showing that Defendants traded on the basis of material nonpublic information that was obtained by hacking into the nonpublic networks of two law firms meets each of the required elements for primary liability under § 10(b) and Rule 10b-5.

*First*, the facts discussed above establish that each of the Defendants directly or indirectly used a fraudulent device to steal material nonpublic information from Law Firm 1 and Law Firm 2. Computer hacking can constitute “a deceptive device or contrivance” prohibited by § 10(b) and Rule 10b-5 when deceptive means are used to accomplish the hack. *See Dorozhko*, 574 F.3d at 51. Here, the hacks into Law Firm 1’s and Law Firm 2’s nonpublic networks were accomplished by deceptive means. With respect to both firms, access to the nonpublic networks was gained by compromising the user accounts of IT employees, posing as those IT employees on the respective firms’ nonpublic networks, and using their credentials to unlock email accounts that contained material nonpublic information. Malware also was used to give commands to the respective law firms’ servers to trick them into doing work necessary to carry out the hacks. Further deceptive means — including falsely naming files to conceal that they contained stolen data — were used to avoid detection by Law Firm 1’s and Law Firm 2’s network security. These deceptive means establish that, for the purposes of § 10(b) and Rule 10b-5, a fraudulent device was used to hack into the nonpublic networks of Law Firm 1 and Law Firm 2 and steal material nonpublic information.

The link between the fraudulent device and these Defendants is established by forensic evidence that connects Defendants to another hack. Defendants possessed proprietary information from a U.S. Robotics Company, which on information and belief, was obtained when the nonpublic network of a U.S. Robotics Company was hacked. Malware used in that hack emanated from the same IP address as malware used in the Law Firm 2 hack. That same IP address also interfaced with Law Firm 1’s server during the same time period that the IP address was directing malware to the U.S. Robotics Company and Law Firm 2. Additionally, a second IP address both deployed malware to the U.S. Robotics Company and received data stolen from

Law Firm 2. The forensic evidence linking Defendants to the deceptive means used in the Law Firm 1 and Law Firm 2 hacks establish that Defendants directly or indirectly used a fraudulent device to steal material nonpublic information from the law firms' nonpublic networks.

*Second*, Defendants acted with scienter. Defendants developed a strategy, based on "Internal Information of US Stock Operations," with "[t]he goal . . . to improve US stock operations and to seize the right time to buy and sell stocks." Defendants stated that "[w]e should focus on a company's . . . M&A news . . . , which usually would cause the stock price to fluctuate significantly within a short period." To carry out this strategy, Defendants targeted Law Firm 1 and Law Firm 2 and Partner A and Partner B because they represent companies in M&As. Defendants went so far as to graph the change in stock prices associated with a deal on which Partner A provided representation. Defendants then strategically purchased securities in companies that were involved in upcoming M&As for which Partner A and Partner B were providing representation.

*Third*, Defendants' fraudulent scheme was in connection with the purchase and sale of securities. After directly or indirectly using a fraudulent device to steal material nonpublic information from Law Firm 1 and Law Firm 2, Defendants accumulated shares in the companies involved in M&A discussions for which Partner A and Partner B were providing representation. Defendants then sold those shares for substantial profits after the M&As were publicly announced. In total, Defendants bought and sold hundreds of thousands of these companies' shares for a profit of approximately \$3 million.

*Fourth*, Defendants committed the fraud through the instrumentalities of interstate commerce. Through email communications, Defendants developed their strategy — to "focus on a company's M&A news" — and identified Law Firm 1 and Partner A as sources of nonpublic

information about “M&A news.” Although residing outside the territorial limits of the U.S., Defendants accessed the U.S. securities markets. Defendants traded online or through Hong Kong brokerages that had relationships with U.S. firms. Defendant Zheng, in some instances, also traded directly through an online account with U.S.-based Scottrade.

These facts establish a prima facie case of primary liability under § 10(b) and Rule 10b-5.

**b. Secondary Liability Under § 10(b) and Rule 10b-5**

The SEC also makes a prima facie case that satisfies each of the required elements for aiding and abetting liability under § 20(e).

*First*, as outlined in Section II.A.1.i. above, there are ample facts to establish a primary violation of §10(b) and Rule 10b-5. The pattern of hacks at Law Firm 1 and Law Firm 2 followed by Defendants’ significant trades in the securities connected to M&A transactions involving Law Firm 1 and Law Firm 2, as well as Partner A and Partner B demonstrate a fraudulent scheme to trade on the basis of material nonpublic information stolen from Law Firm 1 and Law Firm 2.

*Second*, the pleadings detail Defendants’ knowledge of the fraudulent hacking-to-trade scheme. Indeed, Defendants developed the strategy behind the scheme: seize the right time to buy and sell stocks in U.S. companies by learning “internal” information and focus on M&A news that causes short-term increases in stock prices. Defendants’ emails specifically identified Law Firm 1 and Partner A as sources of such internal information about M&A news. Defendants then executed this trading strategy by trading in companies involved in M&A transactions for which Law Firm 1 and Law Firm 2, and Partner A and Partner B were providing representation. Defendants knew (or were reckless in not knowing) why they were developing a



M&A-focused trading strategy and then trading in securities involved in M&A transactions connected to Law Firm 1 and Law Firm 2.

*Third*, the pleadings establish that Defendants provided substantial assistance to the hacking-to-trade scheme. As noted above, they developed the strategy and identified Law Firm 1 and Partner A as potential sources of M&A news that could lead to profitable securities trading.

These facts in their totality establish that Defendants are, in the alternative, secondarily liable for violating § 10(b) and Rule 10b-5.

**c. Primary Liability Under § 20(b)**

The evidence also establishes a prima facie case of primary liability under § 20(b). The same facts that establish the primary and secondary violations under § 10(b) and Rule 10b-5 also establish a primary violation under § 20(b). The evidence that Defendants developed the M&A trading strategy, Law Firm 1 and Law Firm 2 were hacked by deceptive means, and then Defendants executed trades connected to M&A activity involving Law Firm 1 and Law Firm 2 satisfy the elements of § 20(b). That conduct is fraudulent regardless of whether Defendants completed all the steps in the hacking-to-trade scheme or completed some of them “through or by means of any other person.”

\*\*\*\*\*

This record demonstrates that the SEC makes a prima facie case that Defendants primarily or, alternatively, secondarily violated § 10(b) and Rule 10b-5 by deceptively hacking into Law Firm 1’s and Law Firm 2’s nonpublic networks, gaining access to material nonpublic information about impending M&As, and then using that material nonpublic information to trade profitably in the securities of companies traded on U.S. markets. Moreover, the record



demonstrates that the SEC makes a prima facie case that Defendants alternatively violated § 20(b).

**2. The SEC Makes A Prima Facie Case That Defendants Hong and Chin Violated § 14(e) And Rule 14e-3**

The SEC makes a prima facie case that Defendants Hong and Chin violated § 14(e) of the Exchange Act and Rule 14e-3(a) by engaging in fraudulent trading in connection with a tender offer. Section 14(e) provides that:

It shall be unlawful for any person . . . to engage in any fraudulent, deceptive, or manipulative acts or practices, in connection with any tender offer . . . . The [SEC] shall, for the purposes of this subsection, by rules and regulations define, and prescribe means reasonably designed to prevent, such acts and practices as are fraudulent, deceptive, or manipulative.

15 U.S.C. § 78n(e). Based on this provision, Rule 14e-3(a) imposes a “disclose or abstain from trading” requirement, *United States v. O’Hagan*, 521 U.S. 642, 668 (1997), for possessors of nonpublic information about tender offers:

(a) If any person has taken a substantial step or steps to commence, or has commenced, a tender offer (the ‘offering person’), it shall constitute a fraudulent, deceptive or manipulative act or practice within the meaning of section 14(e) of the [Exchange] Act for any other person who is in possession of material information relating to such tender offer which information he knows or has reason to know is nonpublic and which he knows or has reason to know has been acquired directly or indirectly from:

- (1) The offering person,
- (2) The issuer of the securities sought or to be sought by such tender offer, or
- (3) Any officer, director, partner or employee or any other person acting on behalf of the offering person or such issuer, to purchase or sell or cause to be purchased or sold any of such securities or any securities convertible into or exchangeable for any such securities or any option or right to obtain or to dispose of any of the foregoing securities, unless within a reasonable time prior to any purchase or sale such information and its source are publicly disclosed by press release or otherwise.

17 C.F.R. § 240.14e-3(a) (1996).

“One violates Rule 14e-3(a) if he trades on the basis of material nonpublic information concerning a pending tender offer that he knows or has reason to know has been acquired ‘directly or indirectly’ from an insider of the offeror or issuer, or someone working on their behalf.” *United States v. Chestman*, 947 F.2d 551, 557 (1991) (*en banc*) (“Rule 14e-3(a) is a disclosure provision. It creates a duty in those traders who fall within its ambit to abstain or disclose, without regard to whether the trader owes a pre-existing fiduciary duty to respect the confidentiality of the information.”). At the time of the trading, the “offering person” must have taken “substantial steps” toward a tender offer. *See SEC v. Warde*, 151 F.3d 42, 47 (2d Cir. 1998). But “substantial steps” do not require a definitive determination by the offeror that the merger will take the form of a tender offer. *SEC v. Mayhew*, 121 F.3d 44, 53 (2d Cir. 1997).

The SEC makes a *prima facie* case that Defendants Hong and Chin violated § 14(e) and Rule 14e-3. Defendants Hong and Chin traded Borderfree securities when they had nonpublic information about an unannounced tender offer, and Defendants Hong and Chin knew or had reason to know that information was acquired from the emails of Partner B who was “working on behalf of the offeror,” Pitney Bowes. Specifically, Defendants Hong and Chin, directly, indirectly, or through or by means of others, gained access to Law Firm 2’s email server, including the emails of Partner B, who was representing Pitney Bowes in its nonpublic bid to acquire Borderfree. At that time, Pitney Bowes had taken substantial steps toward acquiring Borderfree by tender offer, and those substantial steps were reflected in confidential information in Partner B’s email. Specifically, Partner B’s email contained a draft of the Pitney Bowes-Borderfree exclusivity agreement about ten days before the tender offer was publicly announced. Just hours after access to that information was obtained through the hack, Defendants Hong and

Chin began trading aggressively in Borderfree. From April 29 through the tender offer's announcement on May 5, Defendants Hong and Chin purchased 113,000 Borderfree shares.

This establishes a prima facie case that Defendants Hong and Chin violated § 14(e) and Rule 14e-3.

**3. The SEC Demonstrates A Reasonable Likelihood That Defendants Will Commit Future Violations Of The Securities Laws**

The SEC demonstrates a reasonable likelihood that Defendants will commit future violations of the securities laws. *Materia*, 745 F.2d at 197. The pleadings reveal that Defendants engaged in a large-scale fraudulent scheme to trade on the basis of material nonpublic information obtained by hacking into non-public law firm networks. “Certainly, the commission of past illegal conduct is highly suggestive of the likelihood of future violations. Whether the inference that the defendant is likely to repeat the wrong is properly drawn, however, depends on the totality of circumstances, and factors suggesting that the infraction might not have been an isolated occurrence are always relevant.” *SEC v. Management Dynamics, Inc.*, 515 F.2d 801, 807 (1975).

Here, given the facts and circumstances, the inference that Defendants are likely to repeat their securities law violations is properly drawn. Over the course of 10 months, Defendants directly, indirectly, or through or by means of others stole more than 76 gigabytes of data from two law firms; bought more than 338,000 shares of three companies at a cost of over \$9 million; and sold those shares for approximately \$3 million in profits. Defendants never voluntarily ceased this pattern of illegal activity. For example, Defendants directly, indirectly, or through or by means of others repeatedly accessed Law Firm 2's network and obtained material nonpublic information about M&As involving Partner B's clients.

Given this extensive pattern of hacking and trading, there is a reasonable likelihood that Defendants again will violate the securities laws. This risk of repetition, coupled with Defendants' prima facie violations of Exchange Act § 10(b), Rule 10b-5, and § 20(b), and Defendants Hong's and Chin's additional prima facie violations of Exchange Act § 14(e) and Rule 14e-3, warrant entry of a temporary restraining order.

**B. The SEC Makes The Showing Required To Freeze Defendants' And Relief Defendant's Assets**

The SEC makes the showing required to freeze Defendants' and Relief Defendant's assets. As noted above, "once the equity jurisdiction of the district court properly has been invoked, the court has the power to order all equitable relief necessary under the circumstances," *Materia*, 745 F.2d at 200, including impoundment of assets, *SEC v. American Bd. of Trade, Inc.*, 830 F.2d 431, 438 (2d Cir. 1987). Asset freezes are "ancillary relief to facilitate enforcement of any disgorgement remedy that might be ordered in the event a violation is established at trial." *SEC v. Unifund SAL*, 910 F.2d 1028, 1041 (2d Cir.1990). The purpose of an asset freeze is "to preserve the status quo by preventing the dissipation and diversion of assets," *SEC v. Infinity Grp. Co.*, 212 F.3d 180, 197 (3d Cir. 2000), and thereby ensure "that any funds that may become due can be collected." *Unifund*, 910 F.2d at 1041. "[T]he SEC is entitled upon an adequate showing . . . to an asset freeze sufficient to preserve its disgorgement remedy as well as assets necessary to pay civil monetary penalties." *SEC v. Maillard*, 2014 WL 1660024, at \*4 (S.D.N.Y. Apr. 23, 2014).

To obtain an asset freeze, the SEC "must show either a likelihood of success on the merits, or that an inference can be drawn that the party has violated the federal securities laws." *SEC v. Byers*, 2009 WL 33434, at \*3 (S.D.N.Y. Jan. 7, 2009). This is a lesser showing than required for a preliminary injunction. *See SEC v. Heden*, 51 F. Supp. 2d 296, 298

(S.D.N.Y.1999) (“Unlike a preliminary injunction enjoining a violation of the securities laws, which requires the SEC to make a substantial showing of likelihood of success as to both a current violation and the risk of repetition, an asset freeze requires a lesser showing.” (citations omitted)).

“The plenary powers of a federal court to order an asset freeze are not limited to assets held solely by an alleged wrongdoer, who is sued as a defendant in an enforcement action.” *Smith v. SEC*, 653 F.3d 121, 128 (2011). Rather, “[f]ederal courts may order equitable relief against a person who is not accused of wrongdoing in a securities enforcement action where that person: (1) has received ill-gotten funds; and (2) does not have a legitimate claim to those funds.” *Cavanagh*, 155 F.3d at 136. To obtain an asset freeze against a relief defendant, the SEC must show only that the funds in the relief defendant’s possession are ill-gotten. *Smith*, 653 F.3d at 128.

The pleadings support immediate freezes of all of Defendants’ and Relief Defendant’s assets. Defendants and Relief Defendant are Chinese nationals with accounts at foreign banks and brokerages. Therefore, there is risk that Defendants and Relief Defendant can move their assets beyond this Court’s reach and thereby shield their assets from an order for disgorgement or civil monetary penalties. Further, there is ongoing risk that the assets in the brokerage accounts will be depleted because Defendants are continuing to trade in and transfer money from those accounts.

As detailed in Sections II.A.1, II.A.2, and II.A.3 above, the SEC meets the higher legal standard required to impose a temporary restraining order on Defendants. Therefore, the SEC satisfies without question the lower asset freeze standard. An inference certainly can be drawn

that Defendants violated the federal securities laws with their hacking-to-trade scheme and that the SEC has a likelihood of succeeding on the merits of its claims.

The SEC also carries its burden to show that Relief Defendant, Sou Cheng Lai, possesses ill-gotten gains and all of her assets should be subject to an immediate freeze. Relief Defendant's brokerage account was controlled by Defendant Hong and used to purchase and sell securities in the hacking-to-trade scheme. As a result, the cash and securities that moved through Relief Defendant's brokerage account represent the proceeds of the fraudulent scheme, rather than any funds to which Relief Defendant has a legitimate claim.

Because the SEC meets the requirements for asset freezes, all of Defendants' and Relief Defendant's assets should be frozen immediately to ensure that funds are available to cover disgorgement, prejudgment interest, and civil monetary penalties.

**C. A Repatriation Order Is Necessary And Appropriate Because There Is Good Cause To Believe That Defendants And Relief Defendant Have Assets Outside The United States**

In addition to asset freezes, a repatriation order is necessary and appropriate here because the overwhelming majority of Defendants' and Relief Defendant's known assets are in China or Hong Kong. "[W]here the Court has the authority to order . . . an asset freeze in order to preserve particular funds in anticipation of potential future disgorgement, it also has the authority to order repatriation of assets to effectuate that freeze order. *SEC v. Illarramendi*, 2011 WL 2457734, \* 7 (D. Conn. June 16, 2011). "Ordering repatriation of foreign assets is necessary and appropriate to preserve and keep intact such funds to satisfy future disgorgement remedies." *Id.* The Court may order repatriation when it has good cause to believe that Defendants and Relief Defendants have assets outside the United States that could be subject to an order directing disgorgement or payment of civil monetary penalties. *See, e.g., id.* (ordering repatriation where "the Court has ample cause to believe that assets outside the United States could be subject to an

eventual disgorgement order such that those assets may be necessary to enable effective relief at a later stage”); *SEC v. Universal Consulting Res. LLC*, 2010 WL 4873733, \*2–4 (D. Colo. Nov. 23, 2010) (finding “good cause to believe that the defendants and relief defendant have interests in or ownership of assets outside of the United States that could be subject to an order directing disgorgement or the payment of civil money penalties in this action and that an order requiring repatriation of such assets is necessary”).

A repatriation order is necessary and appropriate here. As set forth in Section II.B above, the SEC meets the standard to freeze Defendants’ and Relief Defendant’s assets. Therefore, the Court has the authority to order Defendants and Relief Defendant to repatriate their assets to effectuate the asset freezes. Further, Defendants and Relief Defendant are Chinese nationals residing in China. Defendants’ trading on the basis of the stolen material non-public information garnered total illicit profits of approximately \$3 million. Currently, approximately \$216,000 remains in the U.S., with \$76,000 in the Hong cash and margin accounts at Interactive Brokers, and approximately \$140,000 in Zheng’s Scottrade account (Sachar Decl. ¶¶114, 115, 116). These are the only known assets the Defendants and Relief Defendant have in the U.S. Defendants’ and Relief Defendant’s other known assets are located in China and the Chinese Special Administrative Regions of Hong Kong and Macau. These assets include foreign brokerage accounts in the names of the Defendants, some of which were used in the alleged fraud, and foreign bank accounts in the names of the Defendants. (Sachar Decl. ¶¶ 7-13, 16-21, 23, 25-27, 29, 30, 32, 33, 36.) On these facts, there is good cause to believe that assets that could become subject to an order for disgorgement or civil monetary penalties are located overseas. Accordingly, a repatriation order is necessary and appropriate here.



**D. An Expedited Discovery Order Is Necessary And Appropriate**

Because the SEC is seeking a temporary restraining order which will expire no more than 14 days after its entry unless renewed or converted to a preliminary injunction, Fed. R. Civ. P. 65(b)(2), an order for expedited discovery is necessary and appropriate here. An expedited discovery order is ancillary relief that is routinely ordered in conjunction with temporary restraining orders that enjoin violations of the federal securities laws. *See, e.g., SEC v. Babikian*, 2014 WL 2069348, at \*1 (S.D.N.Y. Apr. 21, 2014) (noting that the Court previously issued a temporary restraining order and an order to show cause and “ordered expedited discovery, including responses to the SEC’s requests for admissions and interrogatories within three business days”); *Cobalt Family Investors*, 2011 WL 4899909, at \*1 (noting that the Court previously entered an order “allowing the Commission to take expedited discovery in preparing for a hearing on the Order to Show Cause”); *SEC v. Gonzalez de Castilla*, 145 F. Supp. 2d 402, 404 (S.D.N.Y. June 27, 2001) (noting that the Court previously granted a temporary restraining order and issued an order for expedited discovery). The standard discovery timetables under the Federal Rules of Civil Procedure — which generally do not permit any discovery before the Rule 26 conference, Fed. R. Civ. P. 26(d)(1) — will not allow the Commission, in the short time before the temporary restraining order will expire, to take the discovery necessary to determine the scope of Defendants’ fraudulent scheme and the location of its proceeds. In particular, the SEC needs to propound document requests and interrogatories to determine, among other things, the size of Defendants’ and Relief Defendant’s assets and the identity of any other participants in the scheme. Depositions also are necessary to obtain additional evidence on the chain of events in the hacking-to-trade scheme, including the mechanics of the hacks and Defendants’ role in them. Under these circumstances, an expedited discovery order is necessary and appropriate to effectuate the purposes of the federal securities laws.



**E. An Order Prohibiting Destruction Of Documents Is Necessary And Appropriate**

An order prohibiting Defendants and Relief Defendant from destroying documents that relate to them or the hacking-to-trade scheme also is necessary and appropriate here. A preservation order is ancillary relief that the Court is empowered to grant “where necessary and proper to effectuate the purposes of” the federal securities laws. *See Materia*, 745 F.2d at 200. Indeed, orders prohibiting destruction of documents routinely issue with temporary restraining orders that enjoin securities law violations. *See, e.g., SEC v. McGinnis*, 2013 WL 6500461, at \*1 (D. Conn, Dec. 11, 2013) (“[T]his court granted an ex parte emergency temporary restraining order filed by the SEC which: . . . prohibited the destruction or alteration of documents . . . . “); *Cobalt Family Investors*, 2011 WL 4899909, at \*1 (noting that the Court previously entered a temporary restraining order and an order prohibiting the destruction of documents); *SEC v. Cavanagh*, 1998 WL 132842, at \*1 (S.D.N.Y. Mar. 23, 1998) (noting that the Court previously entered a temporary restraining order that, among other things, enjoined defendants from “destroying documents of relevance to the case”).

Here, an order prohibiting destruction of documents is necessary and appropriate to ensure that Defendants and Relief Defendant are preserving discoverable materials. Without such an order, Defendants and Relief Defendant — who are Chinese nationals presumably unfamiliar with the U.S. legal system — may not be aware of their preservation duties that arose when the Commission filed its Complaint. Therefore, to ensure that materials that relate to Defendants, Relief Defendant, and the fraudulent scheme alleged in the Complaint are available in discovery, a preservation order should be granted.

**F. An Order Permitting Alternative Service Of Process Is Necessary And Appropriate**

An order permitting alternative service of process on Defendants and Relief Defendant, pursuant to Federal Rule of Civil Procedure 4(f)(3), is necessary and appropriate here. “The rule gives considerable discretion to the district courts to fashion methods for appropriate international service.” *SEC v. Shehyn*, 2008 WL 6150322, at \*3 (S.D.N.Y. Nov. 26, 2008). The Rule “provides the Court with flexibility and discretion . . . to fit the manner of service utilized to the facts and circumstances of the particular case.” *Anticevic*, 2009 WL 361739, at \*3 (internal citations omitted). Importantly, “[a] plaintiff is *not* required to attempt service through the other provisions of Rule 4(f) before the Court may order service pursuant to Rule 4(f)(3).” *Id.* (citing *Rio Properties, Inc. v. Rio Int’l Interlink*, 284 F.3d 1007, 1015 (9th Cir.2002) (“Rule 4(f)(3) is not . . . in any way dominated by Rule 4(f)'s other subsections; it stands independently, on equal footing . . . . [N]o language in Rules 4(f)(1) or 4(f)(2) indicates their primacy, and certainly Rule 4(f)(3) includes no qualifiers or limitations which indicate its availability only after attempting service of process by other means.”). “Pursuant to Rule 4(f)(3), a Court may fashion means of service on an individual in a foreign country, so long as the ordered means of service (1) is not prohibited by international agreement; and (2) comports with constitutional notions of due process.” *Id.* (internal citations omitted). Service by email is not prohibited by international agreement and “comports with due process where a plaintiff demonstrates that the email is likely to reach the defendant.” *F.T.C. v. Pecon Software Ltd.*, 2013 WL 4016272, at \*5 (S.D.N.Y. Aug. 7, 2013).

Here, service by email meets the requirements of Rule 4(f)(3) and due process with respect to Defendants and Relief Defendant. They all have known email accounts that were used in connection with the fraudulent scheme. When Defendants and Relief Defendant opened the

brokerage accounts used to make the trades at issue in this action, Defendants and Relief Defendant provided their email addresses to the brokerage firms. Defendants Hong, Zheng, and Chin also used the email addresses to communicate with each other in connection with the scheme. For example, Defendant Zheng emailed Defendant Hong a spreadsheet listing mergers and acquisitions that involved Law Firm 1, and Defendant Hong emailed Defendant Chin a list of partners at Law Firm 1. Defendants' and Relief Defendant's use of email in connection with the fraudulent scheme demonstrates that Defendants and Relief Defendant are likely to receive email service, as required to satisfy the requirements of Rule 4(f)(3) and due process.

In addition, an order permitting the Commission to serve Relief Defendant and Defendants Hong and Chin by mail is necessary and appropriate here. *See Exp.-Imp. Bank v. Asia Pulp & Paper Co., Ltd.*, 2005 WL 1123755, at \*4 (S.D.N.Y. May 11, 2005) (finding that service by mail or international courier satisfies the requirements for alternative service under Fed. R. Civ. P. 4(f)(3)). Relief Defendant and Defendants Hong and Chin have current mailing addresses in Macau that were used in connection with the fraudulent scheme. Additionally, Defendant Chin has a current mailing address in Hong Kong that also was used in connection with the fraudulent scheme. Service by mail at these addresses is likely to reach Defendants Hong and Chin and Relief Defendant because they directed the brokerage firms to mail to these addresses financial documents for accounts that are still active.

Additionally, service by mail in Hong Kong and Macau is not prohibited by the Hague Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters ("Hague Convention"). Article 10(a) of that treaty permits service by mail when the foreign country in which service will be received does not object. *See* Hague Convention, art. 10(a), Nov. 15, 1965, 20 U.S.T. 361. ("Provided the State of

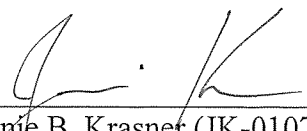
destination does not object, the present Convention shall not interfere with - a) the freedom to send judicial documents, by postal channels, directly to persons abroad[.]” Neither Hong Kong nor Macau has objected to service by mail. *See* Reservations, Declarations, and Understandings for the Special Administrative Region of Hong Kong and the Special Administrative Region of Macao, Hague Convention, available at, <https://www.hcch.net/en/instruments/conventions/statustable/notifications/?csid=393&disp=resn> (last visited Oct. 25, 2016) (including no objection to service by mail under Article 10(a)). Therefore, Relief Defendant and Defendants Hong and Chin may be served by mail in Macau, and Defendant Chin may be served by mail in Hong Kong.

### III. CONCLUSION

For the foregoing reasons, the Commission respectfully requests that the Court grant the SEC’s *Ex Parte* Application For A Temporary Restraining Order And Ancillary Equitable Relief.

Dated: December 27, 2016

Respectfully submitted,




---

Jennie B. Krasner (JK-0107)  
 U.S. Securities and Exchange Commission  
 100 F Street, N.E.  
 Washington, DC 20549  
 (202) 551-4708  
 krasnerj@sec.gov

Britt Biles (*pro hac vice admission pending*)  
U.S. Securities and Exchange Commission  
100 F Street, N.E.  
Washington, DC 20549  
(202) 551-4779  
bilesb@sec.gov  
Attorney for Plaintiff  
Securities and Exchange Commission

Of Counsel:  
Antonia Chion  
Ricky Sachar  
Devon Staren  
Cheryl Crumpton  
U.S. Securities and Exchange Commission  
100 F Street, N.E.  
Washington, DC 20549